APPENDIX F

DATA SECURITY AND CONTROL

A. INTRODUCTION

1. The growing and changing nature of computer-generated and -maintained data is having a major impact in the areas of data security and control in AIS. Ever-increasing amounts of data of greater complexity are being distributed over a wider area at an accelerating rate. To be effective in such an environment, data security and control policies must be implemented in an integrated manner across systems and organizational boundaries. Correspondingly, data administration is challenged to ensure that its area of responsibility is effectively reflected in the development, and implementation, of an integrated data security and control policy. Data administration must ensure that data is accurate and. free from contamination or corruption. This task includes data protection, security, integrity (including synchronization), auditability, and enforcement. Data administration must also ensure its perspective is represented in current policy.

2. Compared to previous methods, current technology, specifically in modern DBMSs, improves access to, and control over, data. This increased access broadens the base of potential users, which increases the risk that unauthorized personnel could obtain sensitive or classified information. Both increased security risks, and the resulting increased access restriction controls, make it imperative that data administration and technical development activities take an active role in supporting system security by designing and employing the additional security capabilities offered by the DBMS. Data administration will be directly involved in the planning and analysis of security controls as they relate to data stewardship and integrity.

a. Stewardship of data, and control exerted by the data steward to establish rules for granting privileges to access items of data in the "system" of DoD databases, is one of the major responsibilities of data administration. Data administration must, therefore, work with customers to resolve all issues to provide maximum functionality and data sharing while at the same time preserving confidentiality and quality of the data being managed.

b. In addition to system security, data administration is responsible for the assurance of integrity, and auditability of data in the system. Data integrity requires verifying that data values conform to the set of allowed values designated for their data types and identifying those data values that do not conform. Data integrity includes the discipline of data synchronization (the timing requirements of, or between, data elements). In addition, data integrity also includes accuracy, consistency, reliability, validity, completeness, and relevancy. Even if the data in a "system" of DoD databases is verified to be correct when the data enters a

database, it still must be protected from unauthorized access and alterations while in the database. Providing for auditability makes it possible to determine the effectiveness of the data protection, security, and integrity procedures of the systems.

B. DATA STABILITY

A critical foundation of an organization's data security and control effort is the stabilization of data both within an organization and across organizational lines. Data stabilization involves the disciplined and precise definition of application-independent data requirements so that the data are subjected to minimal change. When change is required, data stabilization practices hold that the change should be predictable, disrupt the overall data architecture to a minimum degree, and be executed in an auditable manner.

C. DATA SECURITY

Current data security concerns have evolved from a concern for the procedures that use data to the actual data itself. This has focused attention on the idea that data have become an asset with their own integral value. As the way in which we use data undergoes basic changes, so must the approach to data security. The new environment demands that security, including the protection of data subject to use, release, or disclosure restrictions, be implemented in an integrated fashion. Data administration must be proactive in examining all areas of security, including the protection of data subject to use, release, or disclosure restrictions, to ensure that the data administration perspective is properly represented. As data is distributed on a broader scale, there are attendant issues that can only be addressed by an authority with a global view. Data security is no longer a function that is mandated by higher authority and executed within individual systems.

D. DATA CONTROL

Although data control is treated as a separate topic from data security, the two are inextricably bound. Data control will be considered from the perspective of its three major components: data integrity, auditability, and enforcement. Data integrity can be considered the requirement; auditability and enforcement as the tools for ensuring compliance with this requirement.

1. Data Integrity.

Data integrity seeks to ensure that the DBMS will perform its function consistently. That is, it will preserve data without unintentional change, produce results that are correct to the defined degree of precision, maintain data availability, and, whenever possible, allow only a single point-of-entry for the data, regardless of where and how it is used.

a. Data administration's concern for data integrity requires that data values (at the database level) be verified to conform to the set of allowed values designated for their data type. These permitted values arise from the management requirements of the organization.

b. Management requirements are represented in logical models or specifications that guide the development of the physical system or database that will manage the actual values of data stored in databases. However, data integrity, from design to physical management and maintenance, is a common goal of both the physical and logical efforts.

(1) During the design phase, logical data structures need to be developed that ensure that data values can be verified to conform to the specific values, or set of permitted values, designated for their data types.

(2) Data and database integrity focuses on the usage of data. It incorporates the concept of synchronization. In addition, data integrity also includes validity, completeness, and relevancy. Each of the goals of data integrity are briefly defined in Figure F-1, below.

2. Auditability

a. Auditability is the measure of a system's capacity to link defined classes of information across the full breadth of a given environment. From the traditional security perspective, this ability has been most often associated with the management of access control: recording what attempts have been made to access the system and what activities were undertaken upon access being granted. However, as we are increasingly faced with security for distributed systems and inter-organization data, the challenge of auditability has become much broader and more complex.

b. Data administration must establish procedures for auditing individual systems in a manner that balances budget constraints and the reliability of audits. Each system must be mandated to be able to provide a complete description of its metadata in a form defined by the auditing authority and which that authority can automatically process. The system being audited must produce its metadata description in a manner that is as automated as possible so as to ensure that the description is an accurate snapshot of the system as it is currently operating. To ensure data is afforded the appropriate level of security and its integrity is ensured, the data values must be adaptable to their original producer, and metadata must be adaptable to both the source from which it was immediately derived, and also the ultimate authority for that metadata. These audit trails cannot be effectively established unless effective data stability has also been established. The audit trails for metadata and data values should be pursued as two separate, albeit, complementary efforts. To attempt to implement the two concurrently would result in an unnecessarily complex system.

3, Enforcement

Data administration must provide primary support for the enforcement of standards. The data administrator must report any non-compliance with standards to the appropriate authority. Data administration should also be prepared to provide sufficient background information on the circumstances of the non-compliance so that an intelligent judgment can be made by responsible authorities. The application, or system, that is responsible for the non-compliance should be specifically identified and also be able to provide background information to the appropriate authority.

1. Consistency. Data is maintained so that it is free from variation or contradiction.

2. Accuracy. Correct data that conforms to models derived to support enterprise requirements and standards, and user requirements.

3. Timeliness. A condition requiring that a data item or multiple items are provided at the time required or specified.

4. Validity. The quality of maintained data that is found on an adequate system of classification (e. g., data model) that is rigorous enough to compel acceptance.

5. Relevancy. The state of maintaining data in a condition that provides the ability to retrieve the specific information needed by the user.

6. Relatability. The quality of data that permits it to be rationally correlated or compared with other similar or like data.

7. Stability. The ability of a data structure to satisfy additional or changing information needs over time without affecting its original design.

8. Extensibility. The ability of a data structure to accommodate additional values or iterations of data over time without impacting its initial design.

9. Flexibility and/or Modularity. The ability of data structure design to accommodate requirements of change in process without data reengineering or at a minimum not affect major components of the design to accommodate such changes.

Figure F-1. Definitions of the goals of data integrity.